Privacy Auditing and Deduplicating Data With Seccloud In Cloud Computing

K.RAVI PRAKASH
M.Tech Student, Dept of CSE
Brilliant Grammar School Educational Institutions
Group Of Institutions Integrated Campus
Hyderabad, T.S, India

T.RAVINDAR REDDY
Professor, Dept of CSE
Brilliant Grammar School Educational Institutions
Group Of Institutions Integrated Campus
Hyderabad, T.S, India

Abstract: **As the cloud computing technology develops during the last decade, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully trustworthy, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing. In this work, we study the problem of integrity auditing and secure deduplication on cloud data. Specifically, aiming at achieving both data integrity and deduplication in cloud, we propose two secure systems, namely SecCloud and SecCloud+. SecCloud introduces an auditing entity with a maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases.**

SecCloud+ is designed motivated by the fact that customers always want to encrypt their data before uploading, and enables integrity auditing and secure deduplication on encrypted data.

Key Words: **Seccloud; Seccloud+; Integrity Auditing ;Secure De-Duplication; Proof Of Ownership Convergent Encryption;**

I. INTRODUCTION

Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Cloud storage provides customers with benefits, ranging from cost saving and simplified convenience, to mobility opportunities and scalable service. These great properties attract more and more customers to use and storage their personal data to the cloud storage: according to the analysis report, the volume of data in cloud is expected to achieve 40 trillion gigabytes in 2020. Even though cloud storage system has been widely adopted, it fails to accommodate some main emerging needs such as the abilities of auditing integrity of cloud files by cloud clients and detecting duplicated files by cloud servers. We illustrate both problems below. The first problem is integrity auditing. The cloud server is able to relieve clients from the heavy burden of storage management and maintenance. The main difference of cloud storage from traditional in-house storage is that the data is transferred via Internet and stored in an uncertain domain, not under control of the clients at all, which inevitably raises clients great concerns on the integrity of their data. These concerns originate from the fact that the cloud storage is susceptible to security threats from both outside and inside of the cloud and the uncontrolled cloud servers may passively hide some data loss incidents from the clients to maintain their reputation. What is more serious is that for saving money and space, the cloud servers might even actively and deliberately discard rarely accessed data files belonging to an ordinary client. Considering the large size of the outsourced data files and the clients' constrained resource capabilities, the first problem is generalized as how can the client efficiently perform periodical integrity verifications even without the local copy of data files.

II. EXISTING SYSTEM

Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Cloud storage provides customers with benefits, ranging from cost saving and simplified convenience, to mobility opportunities and scalable service. These great features attract more and more customers to utilize and storage their personal data to the cloud storage: according to the analysis report, the volume of data in cloud is expected to achieve 40 trillion gigabytes in 2020.

III. PROPOSED SYSTEM

We determine that our proposed SecCloud system has achieved both integrity auditing and file deduplication. However, it cannot avoid the cloud servers from knowing the content of file s having been stored. In other words, the functionalities of integrity auditing and secure deduplication are only imposed on plain files. In this section, we propose SecCloud+, which grant for integrity auditing and deduplication on encrypted files. System Model Compared with SecCloud, our recommended SecCloud+ involves further trusted entity, namely key server, which is responsible for assigning

clients with secret key (according to the file content) for encrypting files. This architecture is in line with the recent work. But our work is distinguished with the past work by allowing for integrity auditing on encrypted data. SecCloud+ follows the same three protocols (i.e., the file uploading protocol, the integrity auditing protocol and the proof of ownership protocol) as with SecCloud. The only anomaly is the file uploading protocol in SecCloud+ involves an additional stages for communication among cloud client and key server. That is, the client needs to communicate with the key server to get the convergent key for encrypting the uploading file before the phase in SecCloud.

IV. CONCLUSIONS

Aiming at getting both data integrity and deduplication in cloud, we present SecCloud and SecCloud+. SecCloud proposes an auditing entity with maintenance of a MapReduce cloud, which helps clients create data tags before uploading as well as audit the integrity of data having been stored in cloud. In addition, SecCoud enables secure deduplication through ipresenting a Proof of Ownership protocol and avoiding the leakage of side channel information in data deduplication. Compared with previous work, the computation by user in SecCloud is greatly decreased during the file uploading and auditing phases. SecCloud+ is an advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure deduplication directly on encrypted data.

V. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia , ―A view of cloud computing,‖ Communication of the ACM, vol. 53, no. 4, pp.50–58, 2010.

[2] J. Yuan and S. Yu, ―Secure and constant cost public cloud storage auditing with deduplication,‖ in IEEE Conference on Communications and Network Security (CNS), 2013, pp. 145–153.

[3] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, ―Proofs of ownership in remote storage systems,‖ in Proceedings of the 18th ACM Conference on Computer and Communications Security . ACM, 2011, pp. 491– 500.

[4] S. Keelveedhi, M. Bellare, and T. Ristenpart, ―Dupless: Serveraided encryption for deduplicated storage,‖ in Proceedings of the 22Nd USENIX Conference on Security, ser. SEC'13. Washington, D.C.: USENIX Association, 2013, pp. 179–194.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ―Provable data possession at untrusted stores,‖ in Proceedings of the 14th ACM Conference on Computer and Communi cations Security, ser. CCS '07. New York, NY, USA: ACM, 2007.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, ―Remote data checking using provable data possession,‖ ACM Trans. Inf. Syst. Secur., vol. 14, no. 1

[7] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, ―Scalable and efficient provable data possession,‖ in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, ser. SecureComm '08. New York, NY, USA: ACM, 2008.

[8] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, ―Dynamic provable data possession,‖ in Proceedings of the 16th ACM Conference on Computer and Communications Security , ser. CCS '09. New York, NY, USA: ACM, 2009.

[9]. Chanathip Namprempre, Gregory Neven Mihir Bellare, "Security Proofs for IdentityBased Identification and Signature Schemes," Journal of Cryptology,Springer-Verlag, vol. 22, no. 1, pp. 1-61, January 2009.

[10]. H. Wang, "Proxy provable data possession in public clouds," IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.

[11]. Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231– 2244, 2012.

[12]. H. Shacham and B. Waters, "Compact proofs of retrievability," in Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, ser. ASIACRYPT '08. Springer Berlin Heidelberg, 2008, pp. 90– 107.

[13]. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Computer Security – ESORICS 2009, M. Backes and P. Ning,

Eds., vol. 5789. Springer Berlin Heidelberg, 2009, pp. 355–370.

[14]. J. Xu and E.-C. Chang, "Towards efficient proofs of retrievability," in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '12. New York, NY, USA: ACM, 2012, pp. 79– 80.

[15] E. Stefanov, M. van Dijk, A. Juels, and A. Oprea, "Iris: A scalable cloud file system with efficient integrity checks," in Proceedings of the 28th Annual Computer Security Applications Conference, ser. ACSAC '12. New York, NY, USA: ACM, 2012, pp. 229–238.

[16] M. Azraoui, K. Elkhiyaoui, R. Molva, and M. O¨ nen, "Stealthguard: Proofs of retrievability with hidden watchdogs," in Computer Security - ESORICS 2014, ser. Lecture Notes in Computer Science, M. Kutyłowski and J. Vaidya, Eds., vol. 8712. Springer International Publishing, 2014, pp. 239–256.

